

1 Thomas H. Bienert, Jr. (CA State Bar No. 135311, admitted *pro hac vice*)
2 tbienert@bienertkatzman.com
3 Whitney Z. Bernstein (CA State Bar No. 304917 admitted *pro hac vice*)
4 wbernstein@bienertkatzman.com
BIENERT | KATZMAN PC
5 903 Calle Amanecer, Suite 350
6 San Clemente, California 92673
Telephone: (949) 369-3700
7 Facsimile: (949) 369-3701
Attorneys for James Larkin

8 Paul J. Cambria, Jr. (NY State Bar No. 1430909, admitted *pro hac vice*)
9 pcambria@lglaw.com
Erin McCampbell (NY State Bar No. 4480166, admitted *pro hac vice*)
10 emccampbell@lglaw.com
LIPSITZ GREEN SCIME CAMBRIA LLP
11 42 Delaware Avenue, Suite 120
Buffalo, New York 14202
12 Telephone: (716) 849-1333
13 Facsimile: (716) 855-1580
Attorneys for Michael Lacey

14 Additional counsel listed on next two pages
15

16
17 **IN THE UNITED STATES DISTRICT COURT**
18 **FOR THE DISTRICT OF ARIZONA**

19 United States of America,
20

21 Plaintiff.

22 v.

23 Michael Lacey, *et al.*,
24

25 Defendants.
26
27
28

No. CR-18-00422-PHX-SMB

**DEFENDANTS' REPLY IN SUPPORT
OF MOTION TO COMPEL
DISCOVERY (DOC. 643)**

Hearing Date: September 13, 2019
Hearing Time: 11:00 a.m.

Hon. Susan M. Brnovich
Courtroom 506

1 Robert Corn-Revere (D.C. State Bar No. 375415, *admitted pro hac vice*)
robertcornreve@dwt.com

2 DAVIS WRIGHT TREMAINE LLP
3 1919 Pennsylvania Avenue NW, Suite 800
Washington, DC 20006-3401

4 Telephone: (202) 973-4225
5 Facsimile: (202) 973-4499

James C. Grant (WA State Bar No. 14358, *admitted pro hac vice*)
jamesgrant@dwt.com

6 DAVIS WRIGHT TREMAINE LLP
7 920 Fifth Ave, Suite 3300
8 Seattle, WA 98104-1610

9 Telephone: (206) 757-8096
10 Facsimile: (206) 757-7096

Attorneys for Michael Lacey and James Larkin

11 Bruce Feder (AZ Bar No. 004832)
bf@federlawpa.com

12 FEDER LAW OFFICE, P.A.
13 2930 E. Camelback Road, Suite 160
Phoenix, Arizona 85016

14 Telephone: (602) 257-0135
15 *Attorneys for Scott Spear*

16 Gary S. Lincenberg (CA State Bar No. 123058, *admitted pro hac vice*)
glincenberg@birdmarella.com

17 Ariel A. Neuman (CA State Bar. No. 241594, *admitted pro hac vice*)
aneuman@birdmarella.com

18 Gopi K. Panchapakesan (CA State Bar No. 279586, *admitted pro hac vice*)
gpanchapakesan@birdmarella.com

19 BIRD, MARELLA, BOXER, WOLPERT, NESSIM,
20 DROOKS, LINCENBERG & RHOW, P.C.

21 1875 Century Park East, 23rd Floor
Los Angeles, California 90067-2561

22 Telephone: (310) 201-2100
23 Facsimile: (310) 201-2110

Attorneys for John Brunst

24 David Eisenberg (AZ State Bar No. 017218)
david@deisenbergplc.com

25 DAVID EISENBERG, P.L.C.
26 3550 N. Central Avenue, Ste. 1550
Phoenix, Arizona 85012

27 Telephone: (602) 237-5076
28 *Attorneys for Andrew Padilla*

1 Joy Bertrand (AZ State Bar No. 024181)

2 joyous@mailbag.com

3 JOY BERTRAND, ESQ.

4 PO Box 2734

5 Scottsdale, Arizona 85252-2734

6 Telephone: (602) 374-5321

7 Facsimile: (480) 361-4694

8 *Attorneys for Joye Vaught*

1 **I. INTRODUCTION**

2 The government's Opposition to Defendants' Motion to Compel production of a
3 functioning version of the Backpage databases is an exercise in obfuscation. Instead of
4 addressing the issue raised in Defendants' Motion, the government spends pages recounting
5 its purported production of discovery not at issue in this Motion. On the issue that is raised
6 in Defendants' Motion – Defendants' need for and right to functional databases – the
7 government misleads the Court, falsely claiming that it produced the servers in the same
8 condition that "it was seized and received by the government." (Doc. 696 at 14.)

9 The government indicted Defendants for their roles in connection with the website
10 Backpage.com. The government alleges that all adult ads on the website were for prostitution
11 or sex trafficking, that the operations and practices of the site were designed to promote or
12 facilitate this by creating ads for illegal conduct or editing ads to hide illegal conduct, and that
13 Defendants each knowingly participated in this. None of this is true, as evidence concerning
14 actual ads and Backpage's actual practices in screening, blocking, removing, and reporting ads
15 would show. This evidence was available in the Backpage databases and systems as they
16 existed when the government effected its seizures of all the servers beginning in April 2018.

17 The government does not dispute any of this, but instead says that Defendants have
18 had access to "images" of ads and data "in the same format they were received by the
19 government." (Doc. 696. at 7.) Defendants' Motion showed that the government's
20 production of "images" is useless, as it amounts to disjointed data with no functionality to
21 search for related information or to analyze and present cumulative data. *See* Motion at at 9-
22 15 & Exs. H-L (Docs. 643-9 through 643-12). With this reply, Defendants also submit a
23 declaration of Tami Loehrs, an expert in forensic computer evidence, who confirms that the
24 information and data the government has produced to date is not forensically sound and is
25 useless.

26 Pursuant to Defendants' constitutional and statutory rights, this Court should order
27 the production of the databases in the same functioning condition they were in when the
28 government seized them in April 2018.

II. ARGUMENT

a. Defendants Have Sought and Are Entitled To Obtain a Functioning Version of the Backpage.com Website, Databases and Systems.

Defendants' Motion sought production of a functioning version of the Backpage.com website, databases, and systems, as they existed when the government effected its seizures. (Doc. 643.) The government's prosecution of Defendants is based entirely on their connections to the Backpage.com website. The government alleges that all adult ads posted by third parties on the website were for prostitution or sex trafficking, that the operations and practices of the website were designed to promote such illegal conduct, and that Defendants supposedly knew of or participated in this. The government is prosecuting Defendants for the operations and practices of the Backpage.com website. Therefore, the actual website, actual ads as they appeared on the site, actual actions to screen, block and report ads, and the involvement of Defendants (or lack of involvement) is crucially important to this case and the defense. This information was available and readily accessible in the Backpage databases and systems as they existed when the government seized them. In its Response, the government does not dispute any of this.¹

b. The Government's Opposition is Irrelevant to Defendants' Motion.

Defendant's Motion sought "Backpage servers and the databases and material on those servers, in a functional and operational format." Motion at 1. Instead of addressing that issue, the government offers arguments purporting to show that it has complied with discovery obligations generally in ways that have nothing to do with this Motion. Defendants do not agree that the government has complied with its obligations under Rule 16, *Jencks*, *Brady*, or

¹ Indeed, the government has made clear that functionality of the databases is important in this case. As previously noted, the government included in its search warrant application the need to obtain "historical" data and "all versions of an advertisement." (Doc. 643-4 at 12.) In seeking judicial warrants, the government committed that it would take appropriate steps to preserve and not "alter the original evidence" as existed and was accessible on the website, databases and systems. (*Id.*, at 11-12.) Even in its Opposition to the Motion, the government relates that it told Danish authorities "to preserve the servers" there in order "to search and display ads as they would have appeared when the Backpage.com site was active." (Doc. 696 at 6.) The government's argument that Defendants' demand for the functioning Backpage databases is a "fishing expedition," (*Id.* at 9), is utterly disingenuous.

otherwise, but the issues here are not whether the government has produced emails or “hot” documents it claims support its case, nor its production of partial exhibit and witness lists. The issue is the government’s obligation to preserve and produce the Backpage.com website, databases, and systems in a fully useable form – the data and evidence that lies at the heart of this case. The government is prosecuting Defendants for publishing a website and admits that it “seized” that website, but still has not produced it or the data the website and its supporting databases and systems contained.

c. The Government’s Assertions That It Has Produced Actual Data and Ads from the Backpage Website Databases and Systems Are False.

The government tells the Court that it has provided Defendants access to “all of the ads and images . . . in the same format they were received by the government.” (Doc. 696 at 7). This is not true. When the government seized the Backpage servers containing the databases and systems that ran the website, they were operational and functioning. Personnel from Backpage or the government (or anyone with access) could have reviewed all data and information from the website in a complete, fully functional, easily accessible, and useable format and could have searched, tabulated, analyzed, and compared such data. Days after the government disclosed its original indictment, Defendants asked that the website and all data be preserved in a fully-functional format. (Doc. 643-7.) The government has not produced data in that format. As Defendants set forth in the Motion (Doc. 643) and in the attached declaration of Tami Loehrs (Exh. A), an expert in forensic computer evidence, the “imaged” ad data the government extracted from the Backpage servers and produced to Defendants is useless, as the raw database information and image dumps produced bear no resemblance to ads on the website and it is all but impossible to recreate the ads from that data. Moreover, the data is completely disjointed, bereft of any capability to search for related information (*e.g.*, about Backpage’s actions to block ads by a user or to report them to law enforcement, etc.) or to analyze and present cumulative data (*e.g.*, to determine the numbers of ads Backpage blocked and removed in a given period, to show that ad text was not edited, etc.).

The government inaccurately tries to cast Defendants’ Motion as seeking discovery that

1 is different than what the government seized. In reality, the opposite issue is true: the
 2 government is producing the data in a form *different* than it seized it. The government's
 3 suggestions to the contrary seem a deceit on the Court.²

4 **d. The Government Demonstrates That It Violated ESI Protocol.**

5 The government goes even further, suggesting that the “Recommendations for
 6 Electronically Stored Information (ESI) Discovery Production in Federal Criminal Cases” (the
 7 “ESI Protocol”)³ support its position. But the opposite is true. First, the ESI Protocol calls
 8 for the parties to meet and confer about the “mechanics of producing ESI discovery.” ESI
 9 Protocol, Principle 3, p. 2. Here, the government made unilateral decisions about producing
 10 the Backpage I.T. systems data without consulting Defendants, and despite Defendants having
 11 asked days after the original indictment that the website and all data be preserved in a fully-
 12 functional format. (Doc. 643-7.) Second, the ESI Protocol provides that “ESI discovery
 13 should be done in a manner to facilitate electronic search, retrieval, sorting, and management
 14 of discovery information” (ESI Protocol, p. 4)—but the manner in which the government has
 15 unilaterally chosen to produce data from the Backpage I.T. systems does the opposite. Third,
 16 the ESI Protocol calls for producing data in a form that will meet the goals of “retain[ing] the
 17 ESI’s integrity, [] allow[ing] for reasonable usability, and [] reasonably limit[ing] costs” (*Id.*, pp.
 18 9-10)—but the government has produced the Backpage I.T. system data in a manner that
 19 eviscerates the data’s integrity, destroys the data’s usability, and dramatically increases
 20 Defendants’ costs. Fourth, the ESI Protocol provides that “ESI received from third parties
 21 should be produced in the format(s) it was received or in a reasonably usable format(s)” (*Id.*,
 22 p. 17)—but the government has not produced the Backpage I.T. system data in the form it
 23 seized it (functional I.T. systems) or in reasonably usable formats. Finally, although the ESI
 24 Protocol provides that “a party should not be required to take on substantial additional
 25 processing or formatting conversion costs and burdens” (*Id.*, Principle 5, p. 3)—the

26 _____
 27 ² Should the government persist in its claim that it produced the system in the “same
 28 condition it was seized and received by the government,” Defendants request an evidentiary
 hearing to address whether or not the government did so.

³ Available at <http://www.uscourts.gov/sites/default/files/finalesiprotocolbookmarked.pdf>.

government seeks to impose exactly such additional costs and burdens on Defendants by not producing the functional I.T. system. The government's invocation of standard ESI protocols simply highlights its deficient handling of Backpage.com servers and the databases and material that existed on those servers.

III. CONCLUSION

The Court should compel the government to provide access to Backpage.com's systems, servers, databases, and data with the same functionality and in the same condition as they existed at the time of their seizure. The Court should further compel the government to provide the data and information requested in Doc. 643-13, except as disclosure of the Backpage.com servers, databases, and systems may allow Defendants themselves to search, obtain, and collect the requested exculpatory data.

Dated: August 5, 2019

Thomas H. Bienert, Jr.
Whitney Z. Bernstein
BIENERT | KATZMAN PC

By: /s/ Whitney Z. Bernstein
Whitney Z. Bernstein
Attorneys for James Larkin

Dated: August 5, 2019

Paul J. Cambria, Jr.
Erin E. McCampbell
LIPSITZ GREEN SCIME CAMBRIA LLP

By: /s/ Paul J. Cambria, Jr.
Paul J. Cambria, Jr.
Attorneys for Michael Lacey

Dated: August 5, 2019

Robert Corn-Revere
James C. Grant
DAVIS WRIGHT TREMAINE LLP

By: /s/ James C. Grant
James C. Grant
Attorneys for Michael Lacey and James Larkin

1 Dated: August 5, 2019

Bruce Feder
FEDER LAW OFFICE, P.A.

2
3 By: /s/ Bruce Feder
4 Bruce Feder
Attorneys for Scott Spear

5
6 Dated: August 5, 2019

Gary S. Lincenberg
Ariel A. Neuman
Gopi K. Panchapakesan
BIRD, MARELLA, BOXER, WOLPERT, NESSIM,
DROOKS, LINCENBERG & RHOW, P.C.

7
8
9 By: /s/ Ariel A. Neuman
10 Ariel A. Neuman
11 Attorneys for John Brunst

12 Dated: August 5, 2019

David Eisenberg
DAVID EISENBERG, P.L.C.

13
14 By: /s/ David Eisenberg
15 David Eisenberg
16 Attorneys for Andrew Padilla

17 Dated: August 5, 2019

Joy Bertrand
JOY BERTRAND, ESQ.

18
19 By: /s/ Joy Bertrand
20 Joy Bertrand
21 Attorneys for Joye Vaught
22
23
24
25
26
27
28

CERTIFICATE OF SERVICE

I certify that on this 5th day of August 2019, I electronically transmitted a PDF version of this document to the Clerk of the Court, using the CM/ECF System, for filing and for transmittal of a Notice of Electronic Filing to the following CM/ECF registrants listed below.

/s/ Whitney Z. Bernstein

Whitney Z. Bernstein

Anne Michelle Chapman, anne@mscclaw.com
 Erin E. McCampbell, emccampbell@lglaw.com
 Anthony R. Bisconti, tbisconti@bienertkatzman.com
 Ariel A. Neuman, aan@birdmarella.com
 Bruce S. Feder, bf@federlawpa.com
 James C. Grant, jimgrant@dwt.com
 Lee David Stein, lee@mscclaw.com
 Paul J. Cambria, pcambria@lglaw.com
 Robert Corn-Revere, bobcornever@dwt.com
 Ronald Gary London, ronnielondon@dwt.com
 Janey Henze Cook, janey@henzecoockmurphy.com
 John Lewis Littrell, jlittrell@bmkattorneys.com
 Seetha Ramachandran, Seetha.Ramachandran@srz.com
 Thomas H. Bienert, Jr. tbienert@bienertkatzman.com
 Whitney Z. Bernstein, wbernstein@bienertkatzman.com
 Gary S. Lincenberg, glincenberg@birdmarella.com
 Gopi K. Panchapakesan, gpanchapakesan@birdmarella.com
 Michael D. Kimerer, mdk@kimerer.com
 Rhonda Elaine Neff, rneff@kimerer.com
 David S. Eisenberg, david@deisenbergplc.com
 Joy Malby Bertrand, joyous@mailbag.com
 John Jacob Kucera, john.kucera@usdoj.gov
 Kevin M. Rapp, Kevin.Rapp@usdoj.com
 Margaret Wu Perlmeter, Margaret.perlmeter@usdoj.gov
 Reginald E. Jones, reginald.jones4@usdoj.gov
 Peter Shawn Kozinets, Peter.Kozinets@usdoj.gov
 Andrew C. Stone, andrew.stone@usdoj.gov

EXHIBIT A

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

United States of America

Plaintiff,

v.

Michael Lacey, *et al.*,

Defendants.

Case No. CR-18-422-PHX-SMB

DECLARATION OF TAMI LOEHRS

I, TAMI LOEHRS, hereby declare as follows:

Qualifications and Experience

I am a digital forensics expert and owner of Loehrs Forensics, LLC (formerly Loehrs & Associates), a firm specializing in digital forensics. My offices are located at 1505 North Central Avenue, Suite 111, Phoenix, Arizona 85004. I am competent to testify and the matters contained herein are based on my own personal knowledge.

I have been working with computer technology for over 20 years and I hold a Bachelor of Science in Information Systems. I have completed hundreds of hours of forensics training including courses with Guidance Software and Access Data. I am an EnCase Certified Examiner (EnCE), an Access Data Certified Examiner (ACE), a Certified Computer Forensic Examiner (CCFE) and a Certified Hacking Forensic Investigator (CHFI). I have conducted over one-thousand forensics exams on electronic evidence including hard drives, cell phones, removable storage media, security systems, dash cams, and other electronic devices, in addition to forensically preserving and analyzing on-line data such as cloud storage and social media platforms. I have conducted seminars on Computer Forensics and Electronic Discovery throughout the United States. In addition, I hold a Private Investigator Agency

1 License in the State of Arizona which requires a minimum of 6,000 hours investigative
2 experience. My Curriculum Vitae is attached as Exhibit A.

3 I have been hired as a digital forensics expert on over one thousand criminal and civil
4 cases throughout the United States and internationally since the year 2000 and I have
5 testified over one hundred and twenty-six times as a digital forensics expert in State, Federal
6 and international Courts.

7 **Role of Loehrs Forensics**

8 I have been retained as a digital forensics expert by counsel for defendants for the
9 purpose of assisting with matters related to the searching, collecting, analyzing and
10 producing of electronic evidence in this case. Specifically, the government has alleged that
11 Defendants facilitated the promotion of prostitution through the use of the website
12 Backpage.com and conspired to commit money laundering. The government seized
13 approximately one-hundred and six (106) servers associated with the operation of
14 Backpage.com and these servers were located in Tucson, Dallas and Amsterdam. Using
15 industry standard methodologies, techniques and tools, it is the role of Loehrs Forensics to
16 assist defendants in accessing the Backpage.com data that resides on these servers for the
17 purpose of corroborating or refuting the government's allegations.

18 I have reviewed discovery materials produced by the government including, but not
19 limited to, evidence chain of custody forms regarding items collected from 202 S. Tucson
20 Blvd, Tucson, AZ on May 3, 2018, 13601 Preston Road, Dallas, TX on May 10, 2018 and 1855
21 N. 6th Avenue, Tucson, AZ on April 6, 2018; photographs; Joint Status Reports with exhibits;
22 and the Superseding Indictment.

23 On April 17, 2019, I flew to Pocatello, Idaho to review fourteen (14) of the servers in the
24 government's possession. The servers were located on several different tables, with two to
25 three servers stacked on top of each other. During my visit, I was restricted to a visual
26
27
28

1 inspection only and was not permitted to photograph the servers or power them up to
2 determine the configuration of the servers or the nature of the data contained within.

3 On April 23, 2019, I conducted a similar visual inspection of thirty-two (32) servers and
4 three (3) external hard drives located at the FBI in Phoenix, Arizona. Again, I was not
5 permitted to photograph the servers or power them up to determine the configuration of the
6 servers or the nature of the data contained within. Also during that visit, four hard drives
7 containing digital evidence in this matter were released to me for my review and analysis to
8 be conducted at the Loehrs Forensics lab.

9
10 On May 17, 2019, Loehrs Forensics picked up three boxes of evidence from the offices of
11 Bruce Feder and took them to the Loehrs Forensics lab for review and analysis. Those three
12 boxes contain fifty-six (56) hard drives produced by the government that purport to be five
13 (5) of the one hundred and six (106) servers seized from Backpage.com.

14 **Summary of Opinions and Conclusions**

15 The majority of the electronic data seized from Backpage.com and produced by the
16 government does not meet minimum industry standards and is completely unusable in its
17 current form. The issues with the data produced by the government includes, but is not
18 limited to, the way in which the data was acquired and preserved, the integrity of the data
19 produced and the ability or lack thereof to access, review and analyze the data.

20
21 There are nationally and globally accepted standards for documenting, acquiring and
22 preserving digital evidence. Some of the most recognized organizations who promote those
23 standards include the International Organization for Standardization (www.ISO.org), the
24 Scientific Working Group on Digital Evidence (www.SWGDE.org), and the National Institute
25 of Standards and Technology (www.NIST.gov). In addition, law enforcement has adopted its
26 own standards for acquiring and preserving digital evidence. Regardless of the organization
27 or agency setting the standards, the methodologies accepted for acquiring and preserving
28

1 digital evidence are identical in their purpose, to maintain the integrity of the data being
2 acquired and preserved and the government failed to do that in this case.

3 **Backpage.com Operations**

4 Based on my review of SA Robinson's Declaration, Backpage.com relied upon database
5 servers, image servers and web servers to host the website as it would have appeared to users
6 on the Internet. No one server contains web pages as they were presented to the user when
7 the site was active, rather, elements would need to be pulled from multiple servers in order to
8 generate an ad as it would have been displayed to the user. In fact, a single advertisement on
9 the website may be constructed of multiple files spread throughout numerous servers and
10 hundreds of hard drives. Further, any actions taken with regard to an advertisement, such as
11 removing it, would also be located among multiple files, multiple servers and multiple hard
12 drives all working as a cohesive unit. When any one component of the unit has been damaged
13 or removed, the advertisement and any activity associated with that advertisement, may be
14 lost. This includes, but is not limited to:

- 16 • whether the ad was blocked and when,
- 17 • whether the source of the ad was blocked and when,
- 18 • whether the ad was removed from the website and when,
- 19 • whether the ad was reported to law enforcement and when,
- 20 • who accessed an ad on the website and what the result was, and
- 21 • which individuals were involved in any of these activities.

22
23 In that regard, it is critical that all Backpage.com servers are acquired and preserved in
24 such a manner so as not to destroy or remove any one of these components and maintain the
25 data in substantially the same state it was in when it was active on the Internet.

26 **Data Acquisition and Preservation**

27 When electronic data becomes evidence in a case, it is up to the forensic examiner to
28 assess the digital evidence thoroughly to determine the best course of action to take. Digital
DECLARATION OF TAMI LOEHRS - 4

1 evidence is fragile and can easily be altered or damaged. Similar to preserving a crime scene,
2 the investigator must protect potential physical evidence from being damaged or destroyed.
3 The investigator cannot just tread through the bloody crime scene in street shoes and pick up
4 the murder weapon with an ungloved hand, he must assess the situation and plan
5 accordingly. Careful considerations must also be made with regard to the tools to be used at
6 the crime scene, the methods in which to acquire and preserve the physical evidence and
7 careful documentation of the entire process.

8
9 Similar considerations must be made when acquiring digital evidence, especially when
10 that digital evidence consists of a complicated, dynamic system that depends upon multiple
11 interconnected servers to keep a website up and running. The simple act of powering down a
12 server incorrectly may forever alter and destroy the integrity of the data that resides within.
13 In addition to considerations on how to approach the preservation of evidence, industry
14 standards require that digital evidence be acquired and preserved in a forensically sound
15 manner so as not to alter, damage or destroy that data but to maintain the integrity of that
16 data.

17 When seizing and preserving any electronic media, especially a server, careful
18 documentation of its current state, running processes, physically mounted items, and damage
19 should be thoroughly recorded and photographed. Because servers can be extremely volatile,
20 it is imperative to follow best practices and procedures for each server type and scenario. For
21 instance, if a server containing potential evidence is powered on, the current processes,
22 network configuration, encryption keys and memory should be captured prior to powering off
23 in the event it contains information crucial to properly analyzing the physical hard disks.
24 Servers that are located powered on should also be properly powered down using the
25 operating system shut down function prior to dismantling any of the physical disks to avoid
26 data loss or damage. Servers that are located powered off should be carefully documented to
27
28

1 determine if they are connected to a power source, are warm to the touch that may indicate it
2 was recently powered on,

3 The government has provided very little information, if any at all, as it relates to their
4 process of acquiring and preserving the Backpage.com data. In that regard, it is unknown
5 when the data was acquired, what tool or tools it was acquired with, the type of acquisition
6 conducted, who conducted the acquisition, the name or description of the server being
7 acquired, which specific hard drive in the server was acquired, the configuration of the server
8 and/or the hard drive being acquired, whether the data was encrypted or otherwise formatted
9 in such a way that the integrity of the data could be lost, what processes were running,
10 network configurations, verification that the acquisition process was successful or that the
11 data has been verified as an exact duplicate of the original.
12

13 Additionally, most of the data acquired by the government was not produced in an
14 industry standard format and is not forensically sound. This is tantamount to sending
15 someone a document that cannot be opened in Microsoft Word or Adobe, industry standards,
16 because the document was created with an unknown program, and then not informing the
17 person of the program used. Until the unknown program has been identified and obtained,
18 the document remains inaccessible. Because the data produced by the government is not in
19 industry standard formats and the government has provided little to no information
20 regarding their process for acquiring the data, I am unable to access, identify or restore the
21 data to its original condition and the data remains inaccessible and unusable to defendants in
22 its current form.
23

24 **Integrity of the Data**

25 Data integrity refers to the accuracy and consistency of data. Essentially, the data
26 should be in substantially the same condition as it was when it was taken into custody. In this
27 case, the original condition of the Backpage.com data was a working website. That website
28 contained millions of advertisements with images and text that could be viewed on the

1 Internet, but also contained internal data related to the editing, blocking, removal, payment
2 and reporting of those advertisements. The functionality of the Backpage.com website was
3 dependent upon numerous interrelated servers, each server containing multiple internal hard
4 drives that also work together as a cohesive unit. If any one of these servers or any single
5 hard drive within those servers has not been properly acquired and preserved, the
6 Backpage.com website does not function in its original condition.

7
8 The data produced by the government bears no resemblance to the original
9 Backpage.com website and the integrity of that data has been destroyed in a number of ways.
10 First, the government has not produced all of the interrelated servers required for the
11 Backpage.com website to function. Second, the government has not produced valid forensic
12 images of the hard drives contained within each of those interrelated servers making it
13 impossible to recreate a single server in substantially the same condition as it was when it was
14 seized. Third, the government has provided no information regarding the configuration of
15 the servers or the hard drives within making it further impossible to recreate a single server
16 in substantially the same condition as it was when it was seized. The data, as it has been
17 produced by the government, has made it impossible to identify, access or restore the data to
18 its original condition and the data remains inaccessible and unusable to defendants in its
19 current form.

20 **Ability to Access the Data**

21
22 An important element of having industry standards is to ensure the data acquired can
23 be accessed by anyone with the proper tools and expertise. It does not matter how
24 experienced or knowledgeable an expert may be, if data is produced in an unknown format
25 that does not meet industry standards, cannot be accessed using industry standard tools, and
26 no information about that format is provided, the data will be inaccessible and unusable.

27 Although the government produced some of the data using industry standard forensic
28 formats, even that data has proven to be inaccessible and unusable. Many of the forensic

1 images produced by the government are incomplete, invalid and cannot be read by industry
2 standard forensic tools. Although numerous attempts were made at accessing these forensic
3 images, using numerous industry standard tools, none were successful and the data remains
4 inaccessible and unusable in its current form.

5 **Conclusions**

6 The data seized by the government in this case is unique because Backpage.com was a
7 working website that relied upon an extensive, complicated system of interconnected servers
8 in order to function. However, the government did not document the system before taking it
9 down, they did not document their processes for acquiring and preserving the evidence, they
10 did not acquire the devices using industry standard methodologies or formats, and they did
11 not produce all of the necessary data to restore the Backpage.com website. Rather, the
12 government has produced only some bits and pieces of a complex integrated system, some of
13 which are broken, with no documentation or information on how it was running when they
14 seized it or the tools and methodologies they used to acquire it. This is tantamount to buying
15 a large piece of unassembled furniture but realizing you don't have all the parts, or the
16 instructions on how to build it, or pictures of the final product, or the specialty tools required
17 for the proprietary hardware required to put it all together.
18

19 The data seized from Backpage.com and produced by the government is undocumented,
20 incomplete, broken, inaccessible and unusable. In its current form, the data produced by the
21 government does not meet industry standards and the integrity of the data has been altered
22 and/or destroyed.
23

24 DATED August 5, 2019.

25 

26
27

Tami Loehrs, CCFE, CHFI, EnCE, ACE
28